



COMPACFLT - EDAC

Enterprise Dynamic Access Control (EDAC)

Point of Contact:
Richard Fernandez
(808) 474-9270



Approved for public release; distribution is unlimited.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2005		2. REPORT TYPE		3. DATES COVERED 00-00-2005 to 00-00-2005	
4. TITLE AND SUBTITLE Enterprise Dynamic Access Control (EDAC) (Briefing Charts)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Space and Naval Warfare Systems Center San Diego, Code 20012, San Diego, CA, 92152				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 40	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



COMPACFLT - EDAC

For licensing information contact:

Stephen Lieberman

Voice: (619) 553-2778

Mobile: (619) 606- 5940

Email: stephen.lieberman@navy.mil

For comments regarding this product contact:

Richard Fernandez

Voice: (808) 474-9270

Email: richard.r.fernandez@navy.mil



Outline

Access control background

Access control lists

Groups

NIST RBAC standard

SEAC RBAC

Customer furnished and maintained assets

How it works

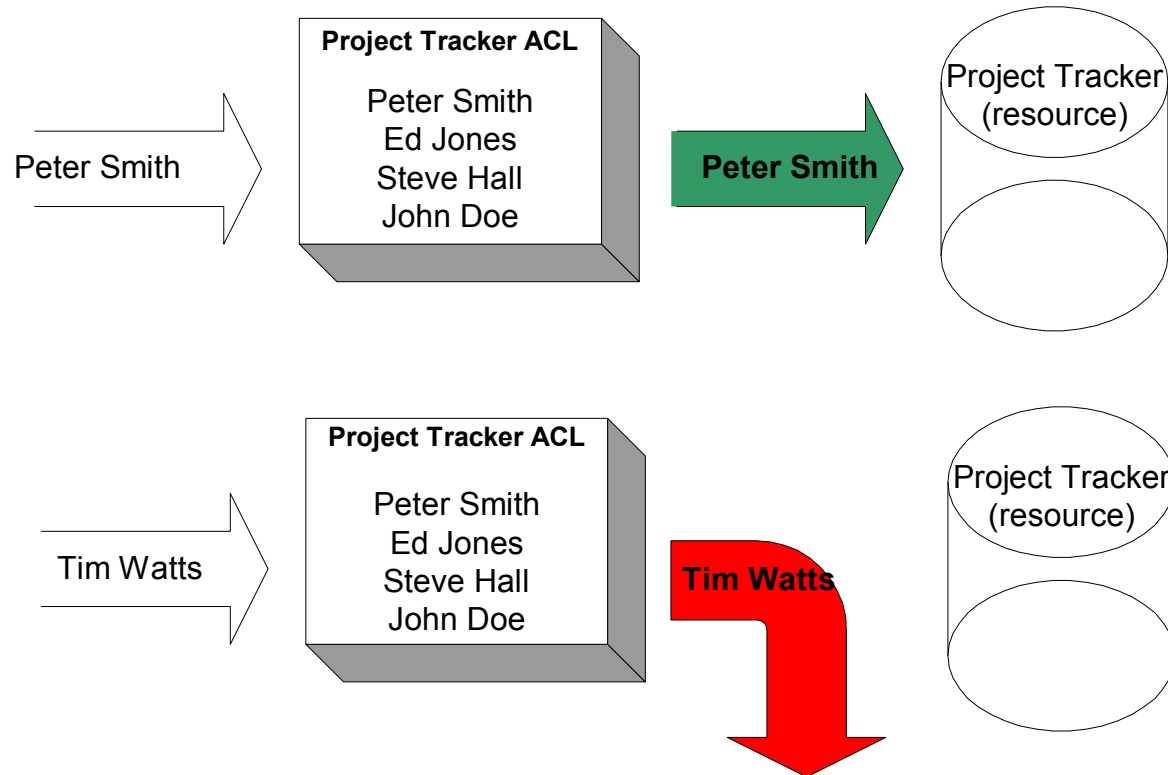
Product overview

Interoperability



Access Control Lists (ACL)

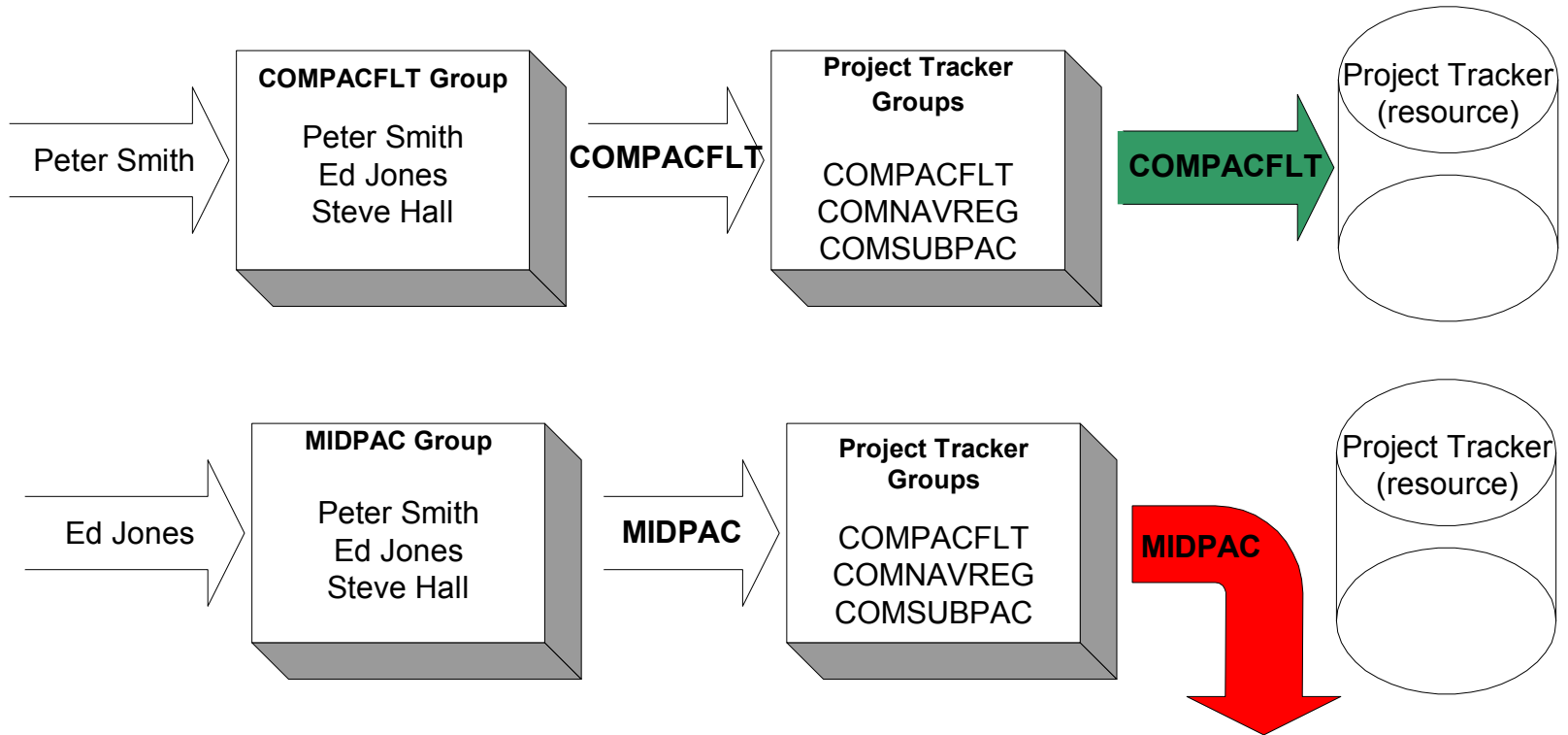
User name or unique identifier associates access to resources





Groups

User associated to a group and group associated to resources





Essentials for resource access

Necessary requirement to access resources:

- Not a user name
- Not a unique identifier
- Not a group association

- List of user characteristics



What are user characteristics

User characteristics (user profile)

- Where client works: **organization**
- What security credentials: **clearance**
- What pay category: **pay grade**
- What branch : **service**
- What vocation: **job function**
- etc



Examples of User Profiles

- User profile is a unique list of user characteristics.
- A client may have more than one user profile.
- User attributes should be compiled from an authoritative data source(s) on a real-time basis.

<u>Categories</u>	<u>COMPACFLT</u>	<u>USNR</u>
Organization:	CPF N65	Naval Intel
Clearance:	Secret	Top Secret
Paygrade:	DP3	02
Service:	DoD	DoNR
Function:	Program Manager	Intelligence



Impact on resource access

The following can affect resource access:

- Transfer to another organization
- Loss of security clearance
- Change in job title
- Job promotion

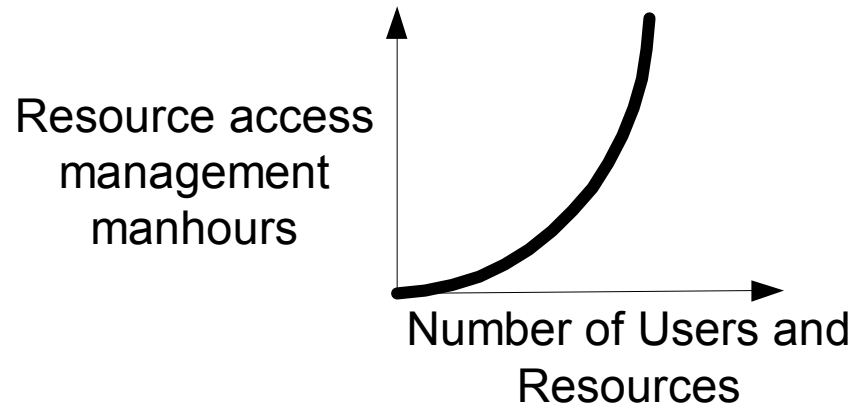


Problems with ACLs and Groups

Maintaining an updated ACL or group is time consuming.

Situation worsens when:

- Number of users increase
- Number of resources increase





NIST RBAC compliance

Because of ACL and group limitations:

The National Institute of Standards and Technology (NIST) RBAC is an American National Standard - ANSI INCITS 359-2004 (approved 19 Feb 04)



NIST RBAC standard

Definitions:

Users and Roles: *"...access decisions are based on the roles that individual users have as part of an organization.*

"Access rights are grouped by role name..."

Role hierarchies: *"Under RBAC, roles can have overlapping responsibilities and privileges;*

Roles and Operations: *"Organizations can establish the rules for the association of operations with roles.*



Access control comparison

How access control solutions can simultaneously evaluate user characteristics.

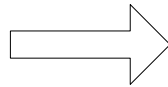
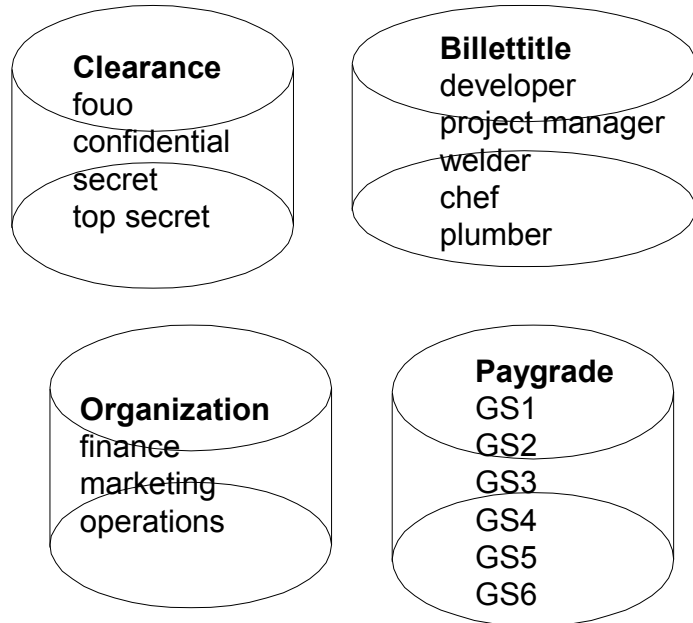
	Simultaneous evaluation of multiple object characteristics & environmentals	Simultaneous evaluation of multiple object characteristic & environmental hierarchies	Real-time detection of object characteristic changes, thus affecting resource access
ACLs	0	No	No
Groups	1	No	No
EDAC	Unlimited	Yes	Yes



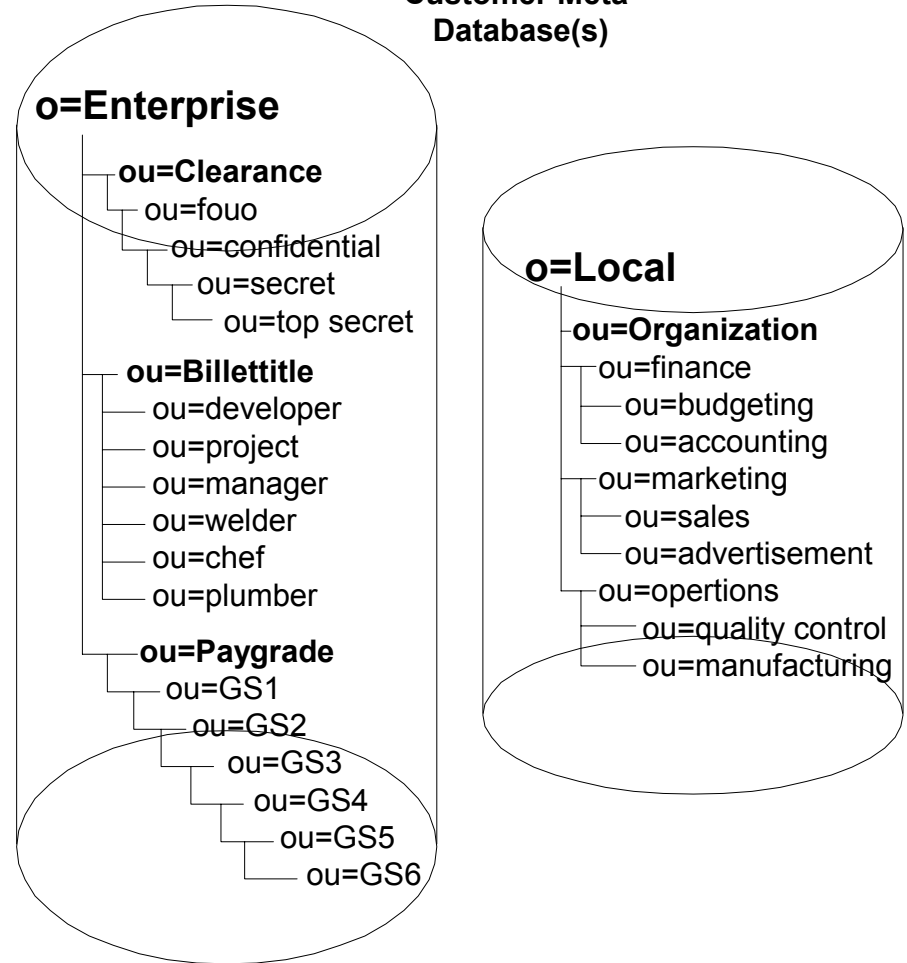
Customer meta-database background

Relational database data duplicated on a directory service.

Customer Personnel Database(s)

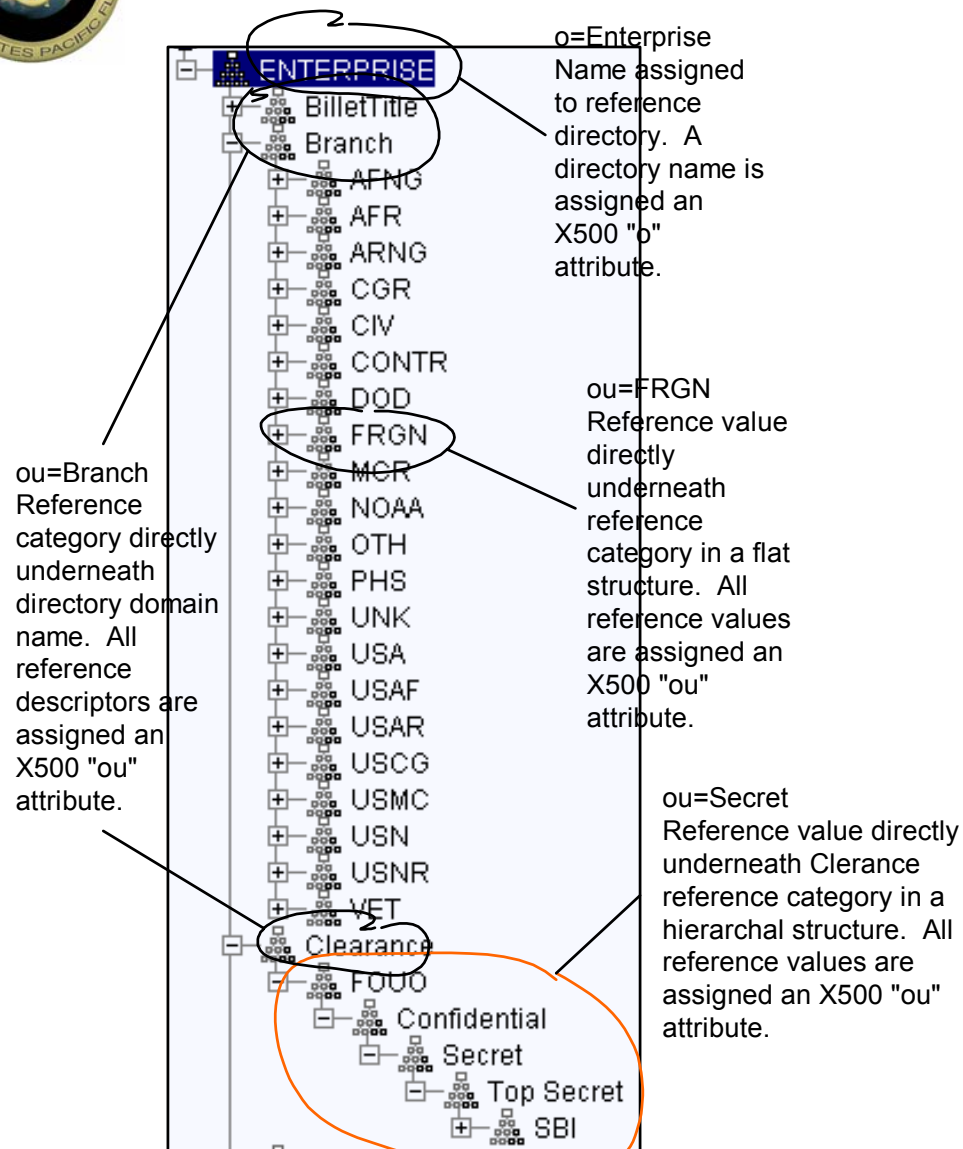


Customer Meta-Database(s)





Customer meta-database specifications

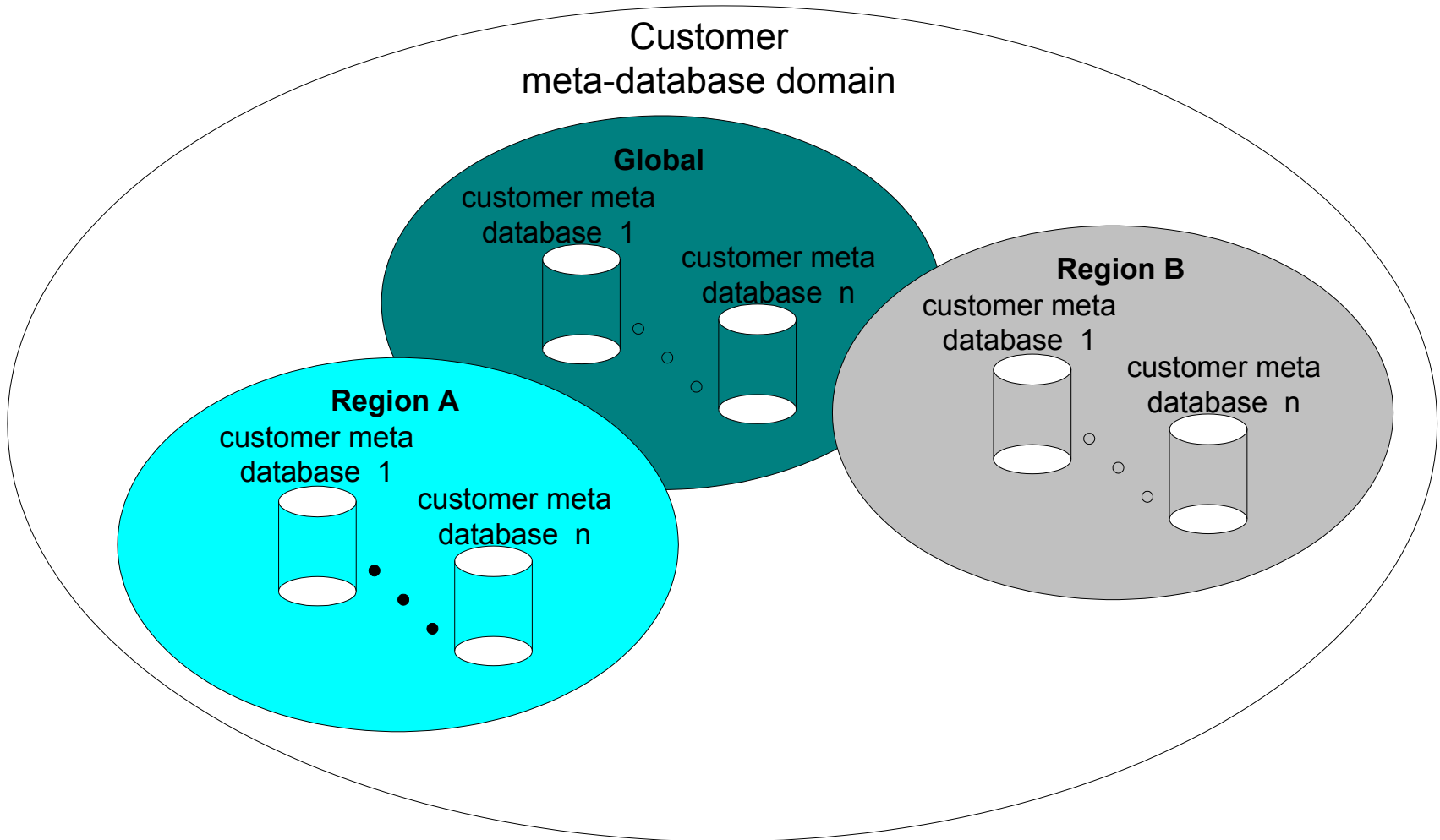


- Customer meta-database
- LDAP v 3/DSML directory
- X500 class objects
 - organization
 - organizationalUnit
- Scalable
 - unlimited entries
 - modifications allowed
- Structure designation
 - domain
 - reference category
 - values
- Structure
 - flat
 - hierarchal
- Maintained
 - local commands
 - regional commands



Customer meta-database domain

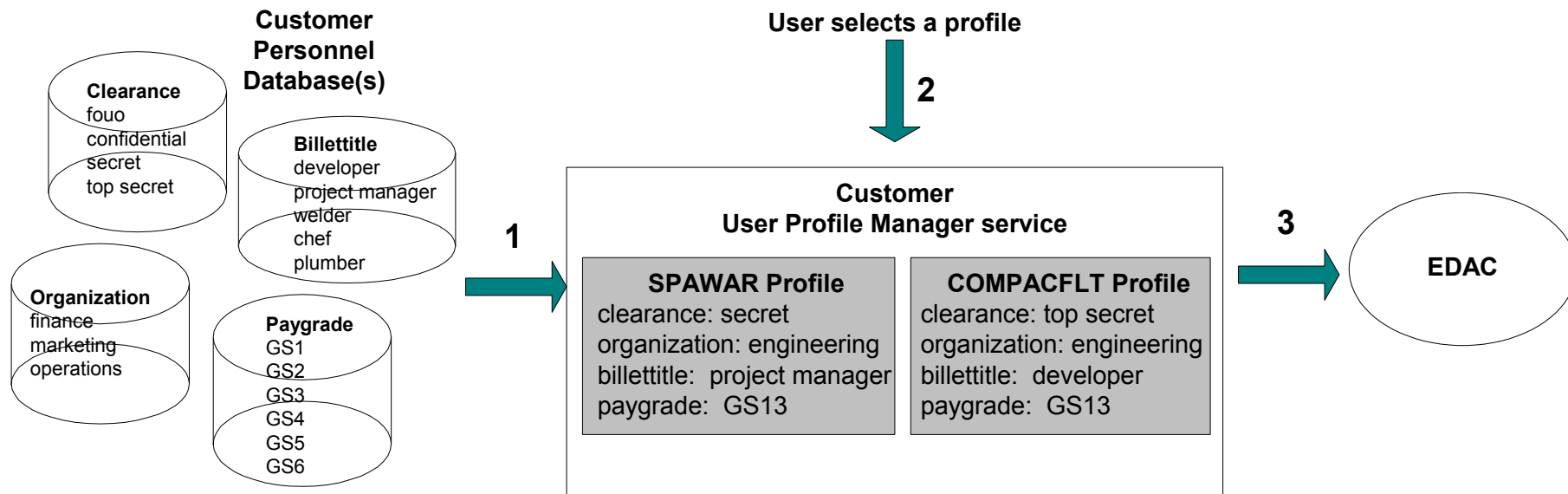
Domain consist of global and regional directories.





User Profile Manager

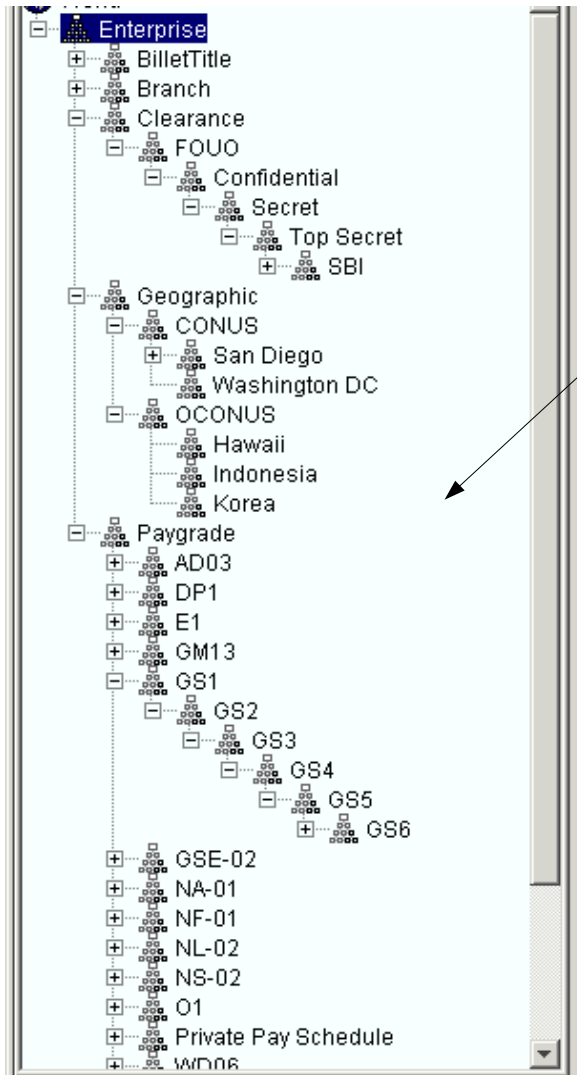
User selects a profile to determine resource access.
Mgmt constraints on user profile selections





How the EDAC works

Customer Meta-Database



RBAC Condition Manager



Step 1:

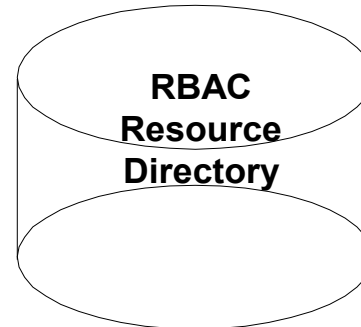
Resource manager establishes a set of conditions to access a resource.

These set of conditions represent a **resource profile**.

Resource Profile

✔ ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
✔ ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

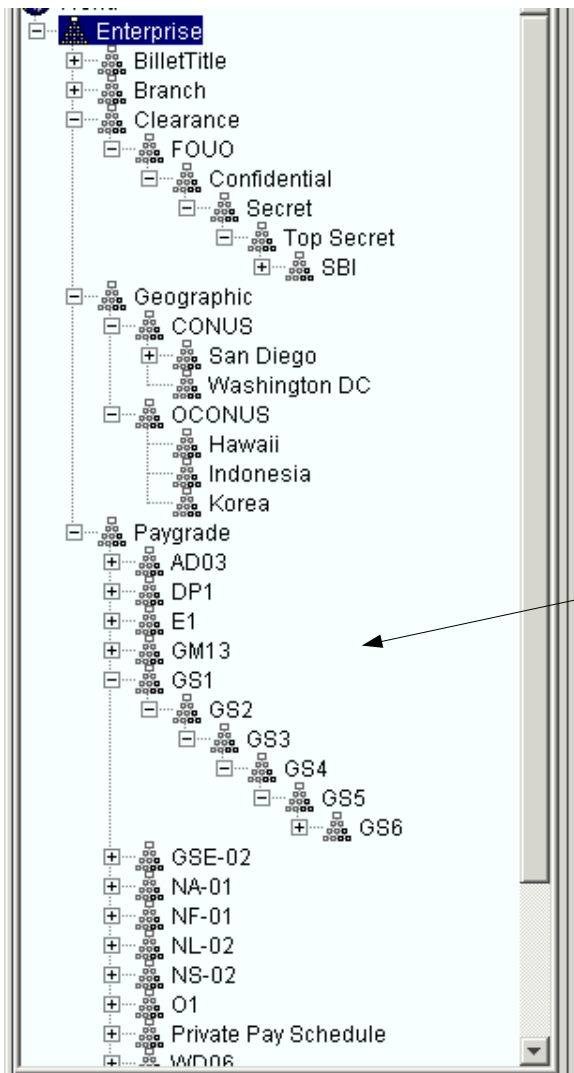
RBAC Resource Directory





How the EDAC works

Customer Meta-Database



Customer User
Profile Manager
Interface



Structure
Format
Service

Step 2:

An effective RBAC requires real-time creation of user profile(s) from authoritative data source(s).

Customer Personnel
Database

Reference Categories	Attributes
assignedCommand	N65
clearance	Secret
paygrade	GS3

User Profile

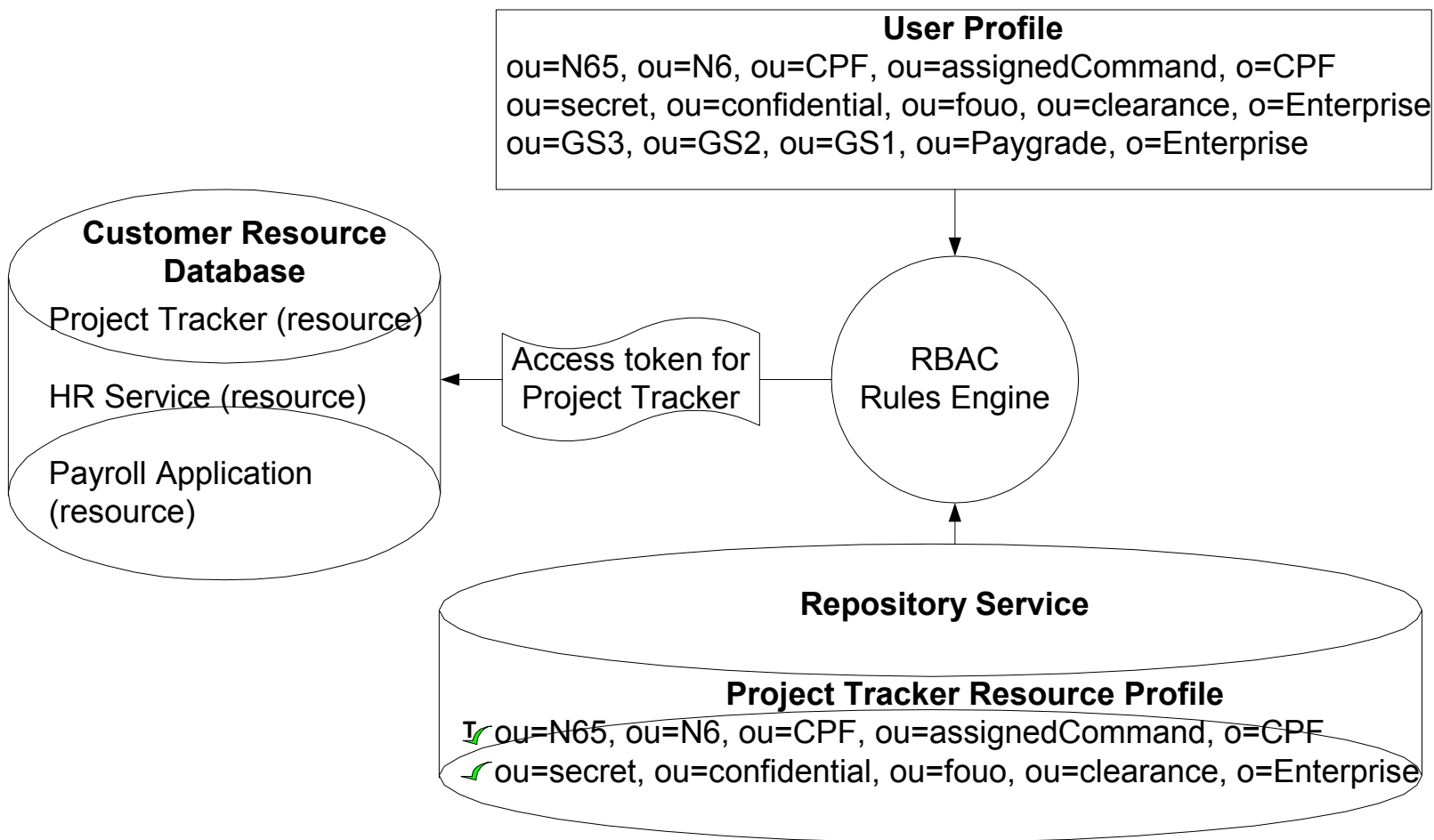
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise



How the EDAC works




Step 3:

The RBAC Rules Engine compares User and Resource Profiles to determine resource access.





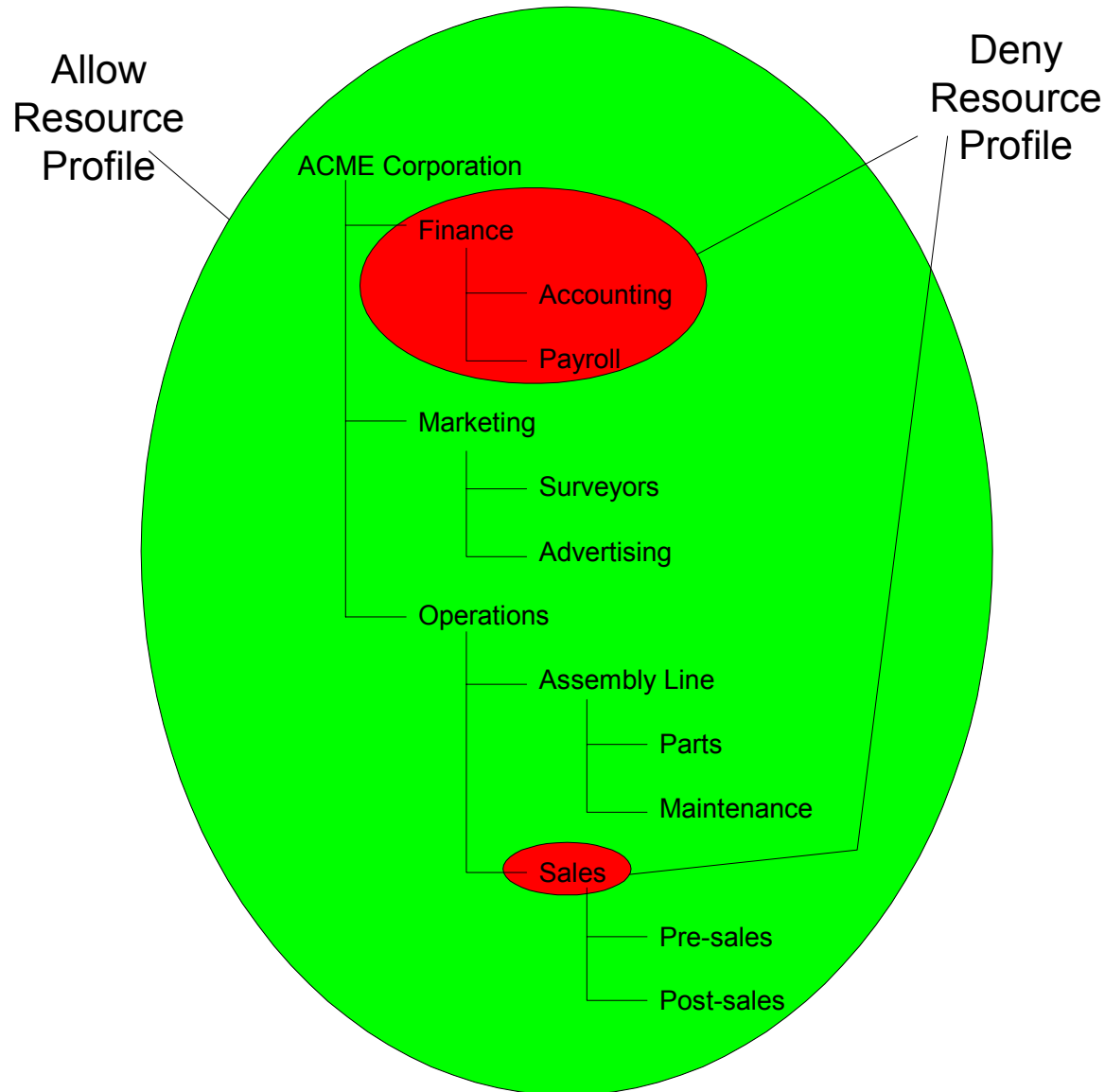
EDAC – Resource profiles

Resource Roles for Project Tracker	Resource Profiles		
Guest	CPF Guest T ✓ COMPACFLT	CSP Guest T ✓ COMSUBPAC ✓ DoD	CNR Guests T ✓ COMNAVREG  Tuesdays 1700 -2300
User	CPF N6 Users T ✓ CPF N6 T ✓ GS12  Mon & Thurs 0800 -1300	Deny Contr Users T ✗ CPF N6 ✗ Secret ✗ CONTR	
Administrator	CPF Admin ✓ CPF N65 T ✓ TS	Deny CPF N65 Admin T ✗ CPF N65 ✗ CONTR  Mon & Thurs 0800 -1300	

- Resource roles
- Allow & Deny profiles
- Exact and subtree conditions
- Time constraints



EDAC – Resource profiles





EDAC – Security levels

During INFOCON B

INFOCON A	Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users		
Admin	CPF Admin	Deny CPF NIS Admin		

INFOCON B

Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users	
Admin	CPF Admin	Deny CPF NIS Admin	

INFOCON C

Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users	
Admin	CPF Admin	Deny CPF NIS Admin	

INFOCON D

Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users	
Admin	CPF Admin	Deny CPF NIS Admin	

During INFOCON C

INFOCON A	Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users		
Admin	CPF Admin	Deny CPF NIS Admin		

INFOCON B

Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users	
Admin	CPF Admin	Deny CPF NIS Admin	

INFOCON C

Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users	
Admin	CPF Admin	Deny CPF NIS Admin	

INFOCON D

Guest	CPF Guest	CSP Guest	CNR Guests
User	CPF NB Users	Deny CNR Users	
Admin	CPF Admin	Deny CPF NIS Admin	

- Pre-configure conditions under each security level.
- RBAC Rules Engine evaluates only conditions for prevailing security level.



EDAC – Model

EDAC standard initiative:

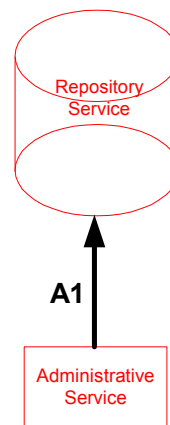
- Interchangeable modular access control components
- Minimum salient features
- Protocol between components
- Standard tie-ins between customer assets and access control system



EDAC - Model

Customer furnished and
maintained assets

Enterprise Dynamic
Access Control (EDAC)

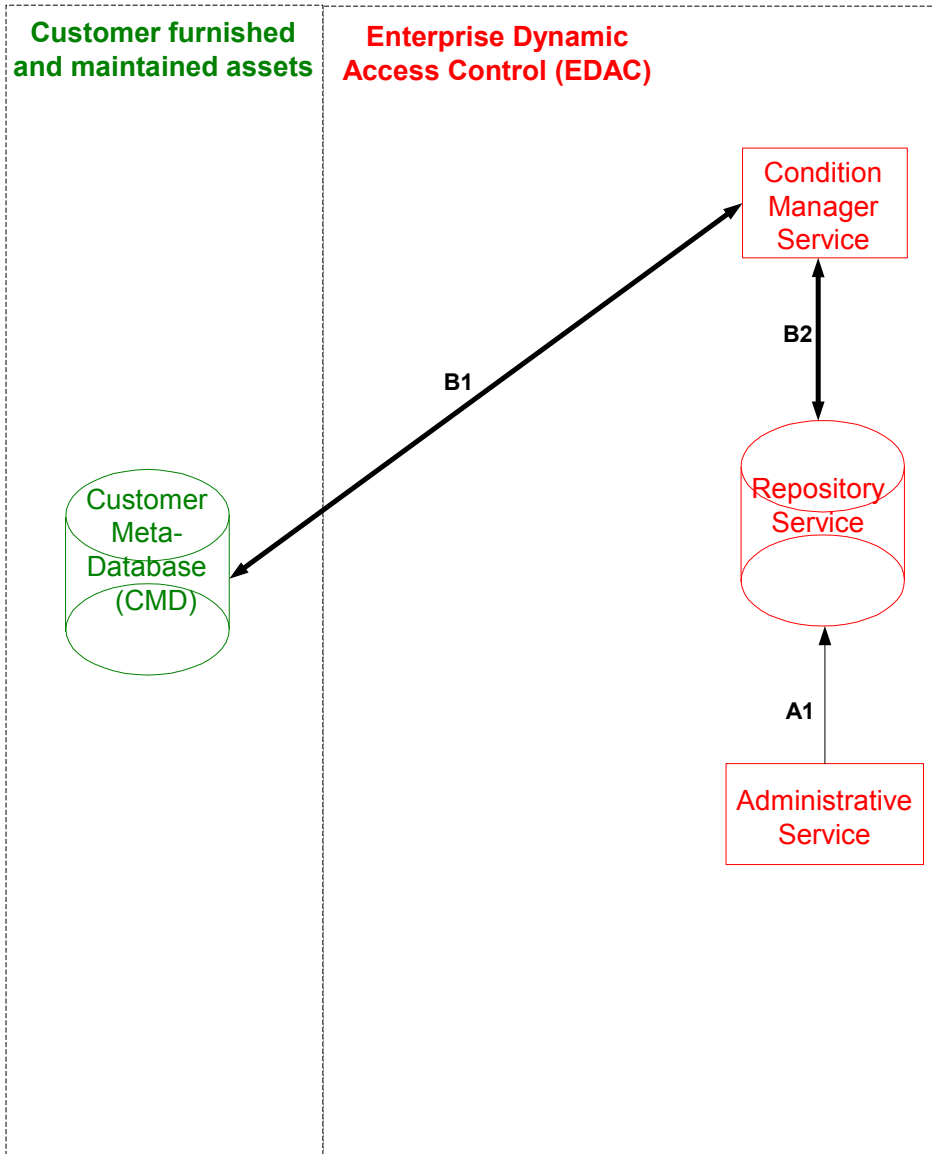


EDAC Process

(A) Administrative Service -
establishes resource
containers, CMD referrals,
RM accounts.



EDAC - Model



EDAC Process

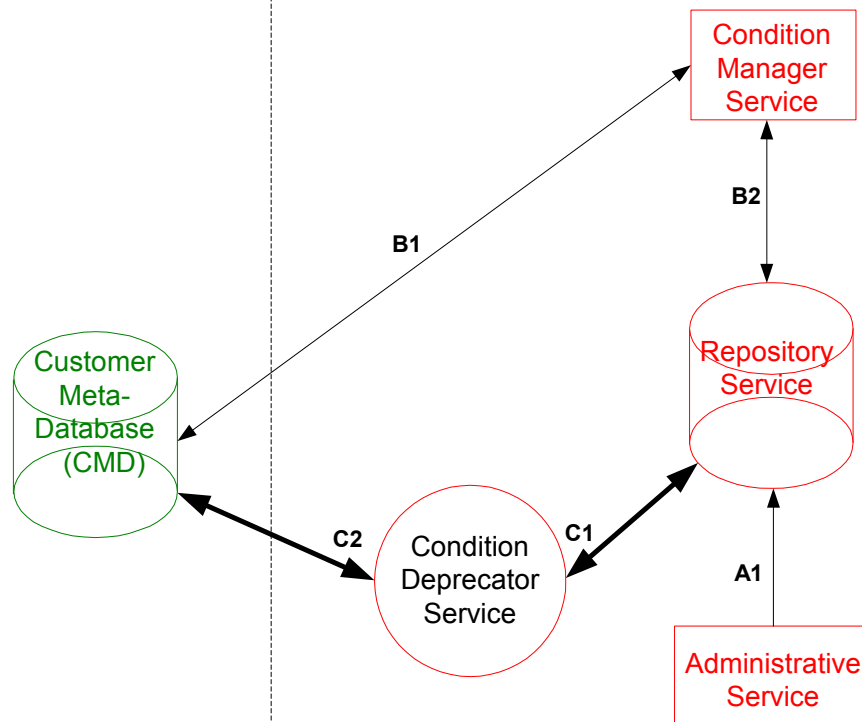
(B) Condition manager Service - Establishes and edits conditions to access resources.



EDAC - Model

**Customer furnished
and maintained assets**

**Enterprise Dynamic
Access Control (EDAC)**



EDAC Process

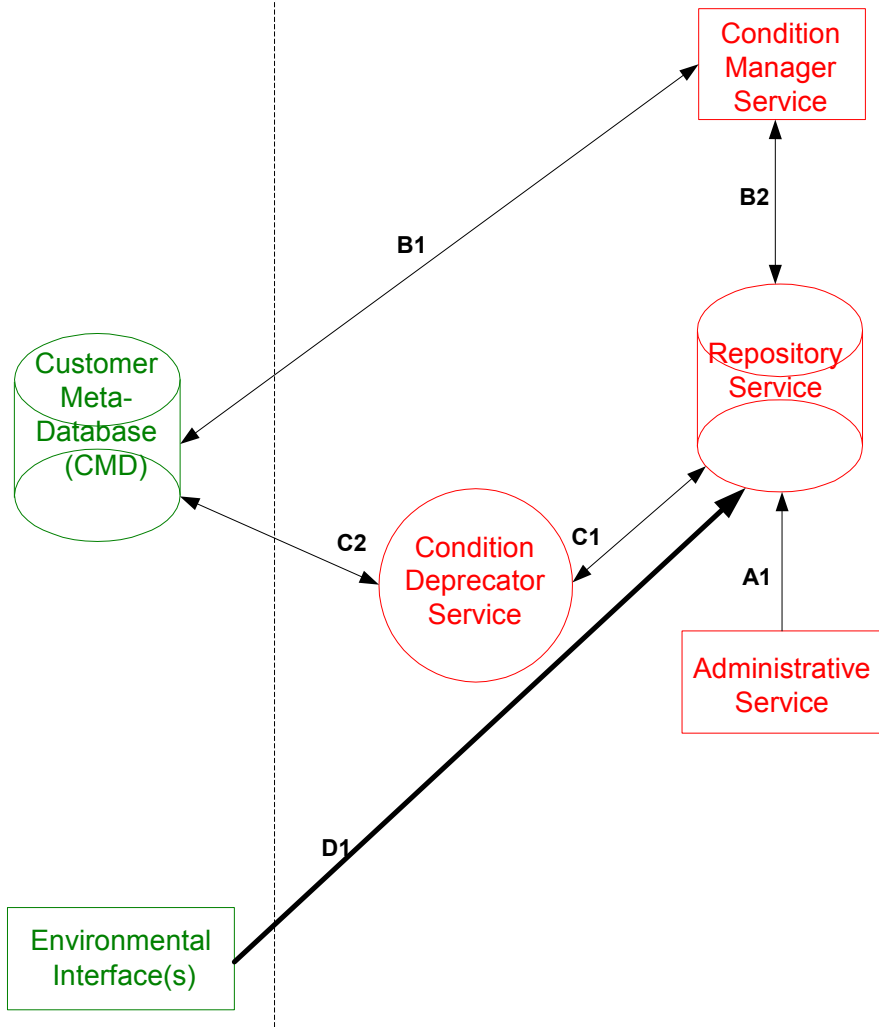
(C) Condition deprecator Service - listens for CMD content changes and flags unmatched or unreachable conditions.



EDAC - Model

**Customer furnished
and maintained assets**

**Enterprise Dynamic
Access Control (EDAC)**

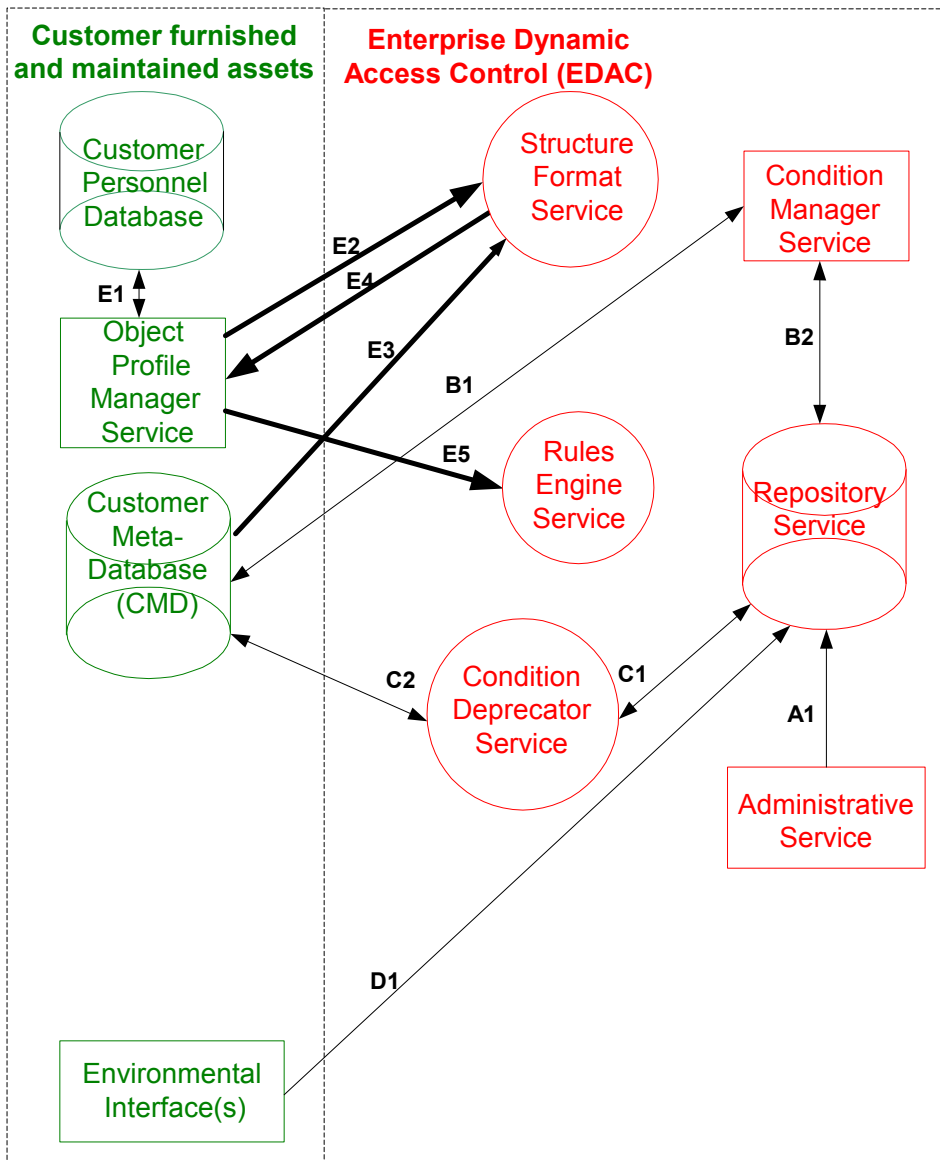


EDAC Process

(D) Customer
Environmental Interface
- furnishes
environmental updates.



EDAC - Model

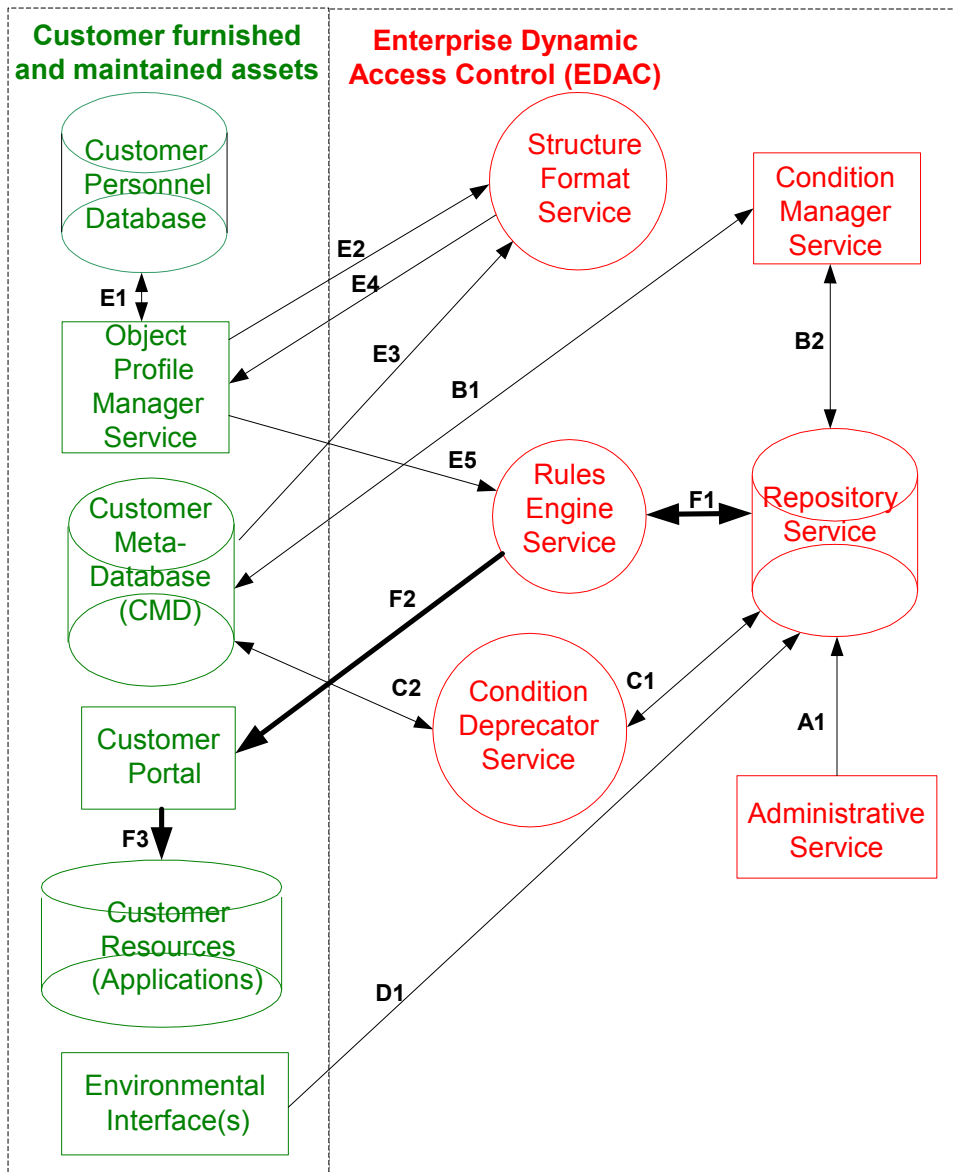


EDAC Process

(E) Customer Object profile manager Service
- object characteristic compilation, selection and formatting.



EDAC - Model



EDAC Process

(F) Rules Engine Service - evaluates object and conditions to determine object resource access.



EDAC – Interoperability

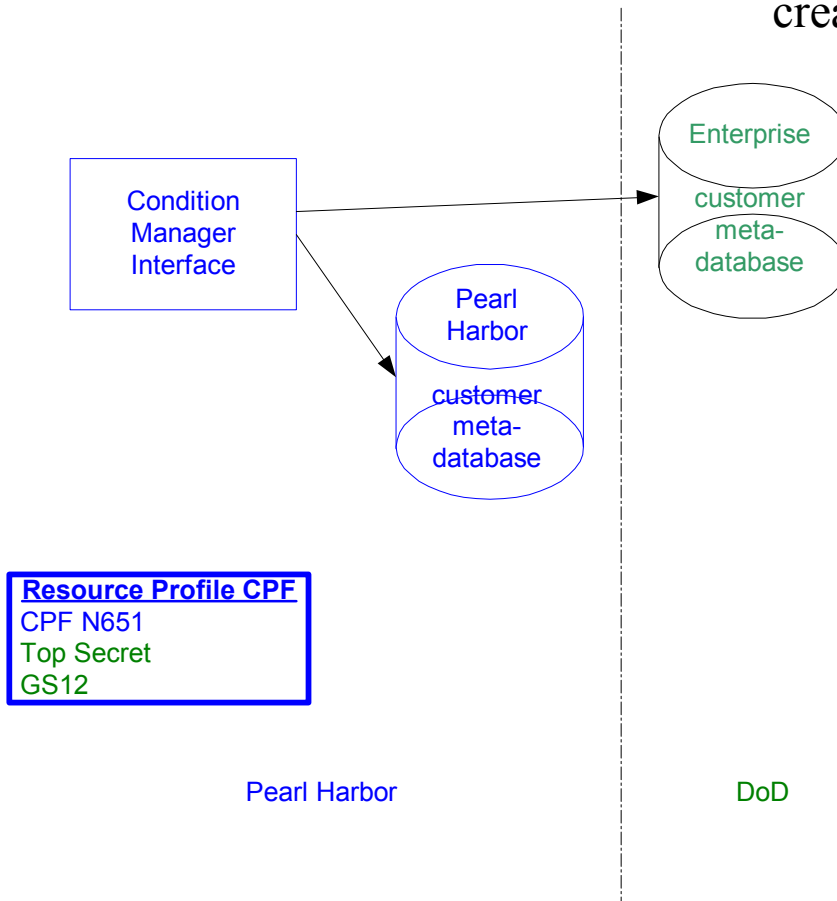
EDAC interoperable among regions:

- Set conditional access for remote users
- Domain customer meta-databases



EDAC - Interoperability

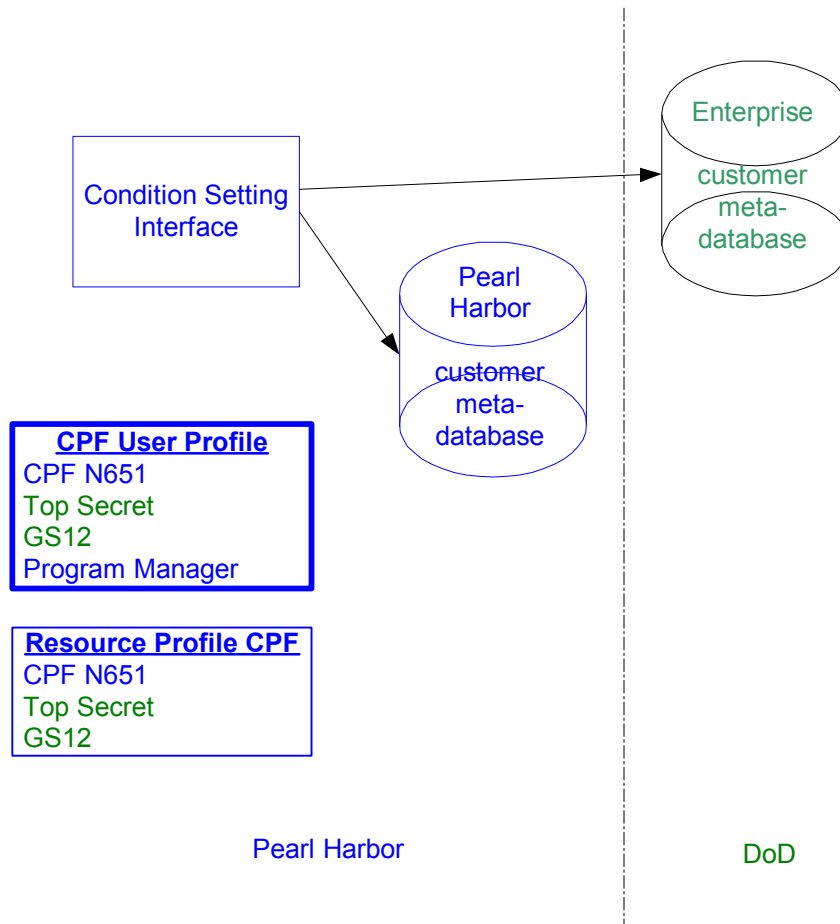
Pearl Harbor: resource profile created for local resource access.





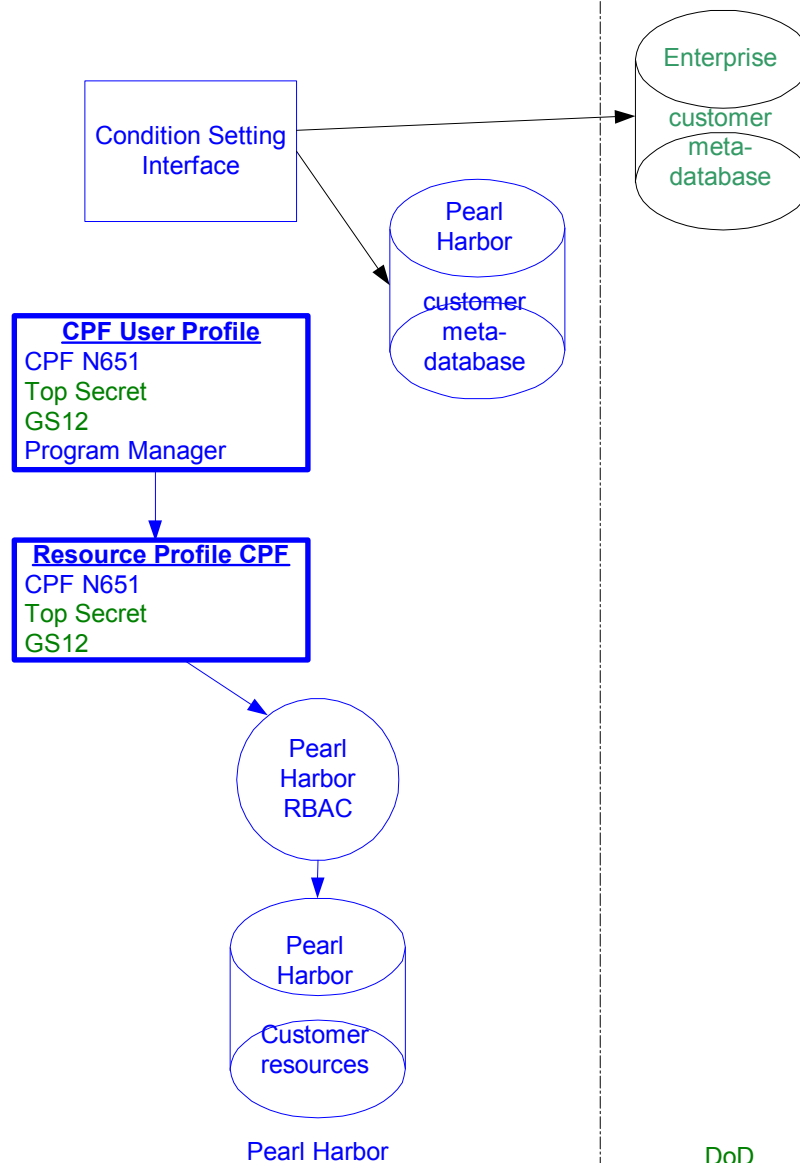
EDAC - Interoperability

Pearl Harbor: local user profile is generated to access a local resource.





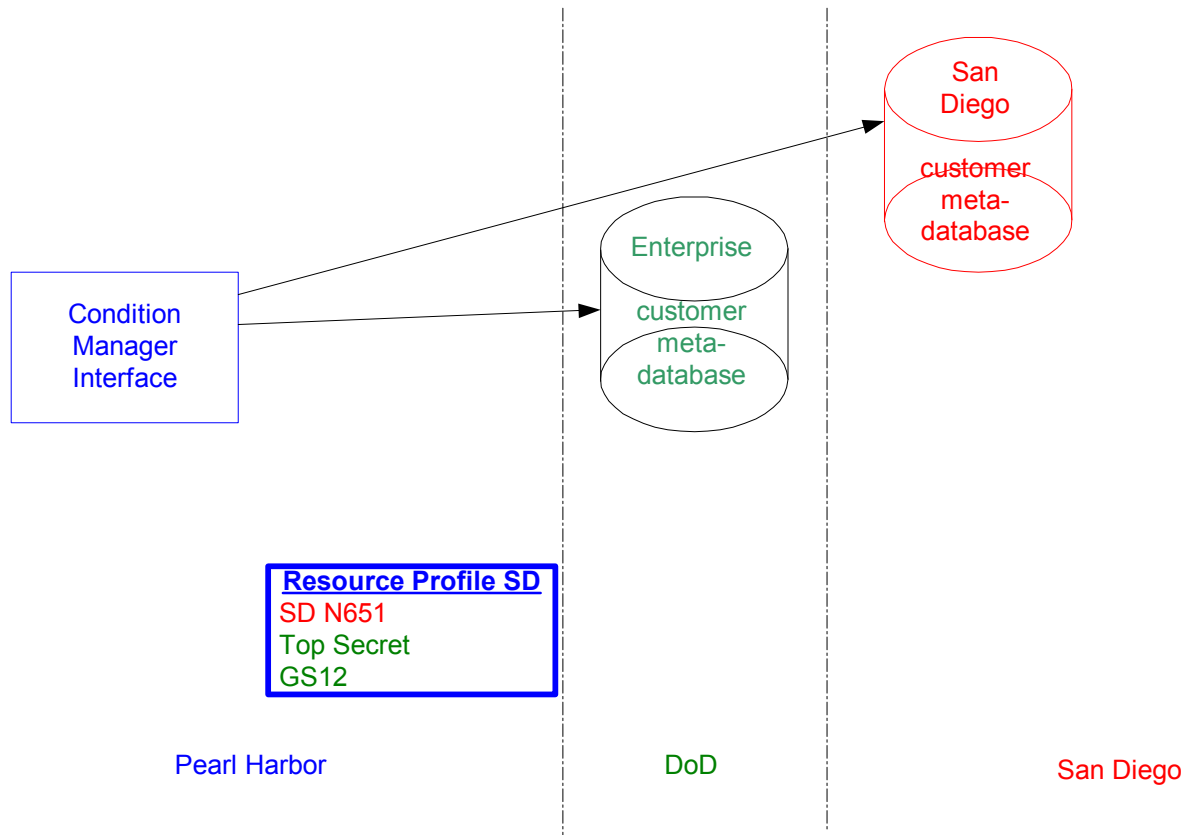
EDAC - Interoperability



Pearl Harbor: user and resource profiles are evaluated by rules engine to determine local resource access.



EDAC - Interoperability

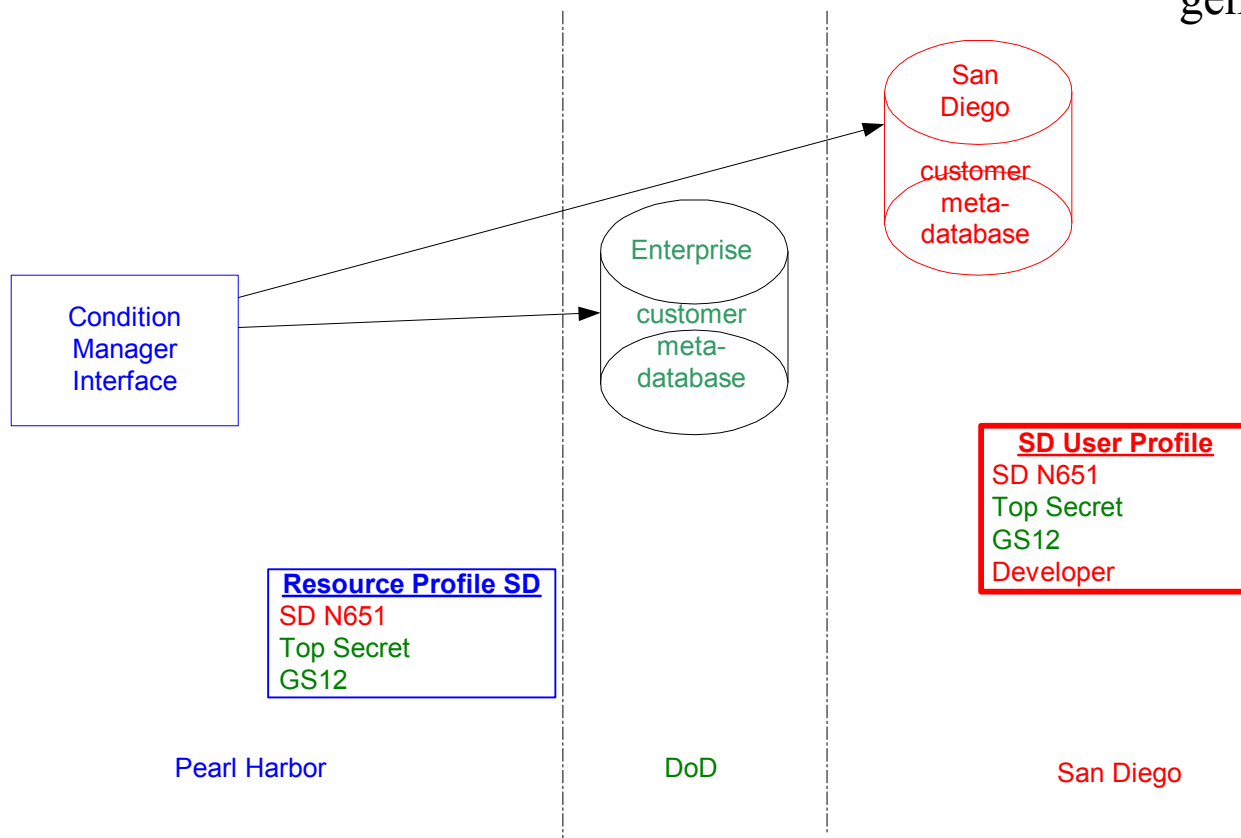


Pearl Harbor: A resource profile to allow remote users access to local resources.



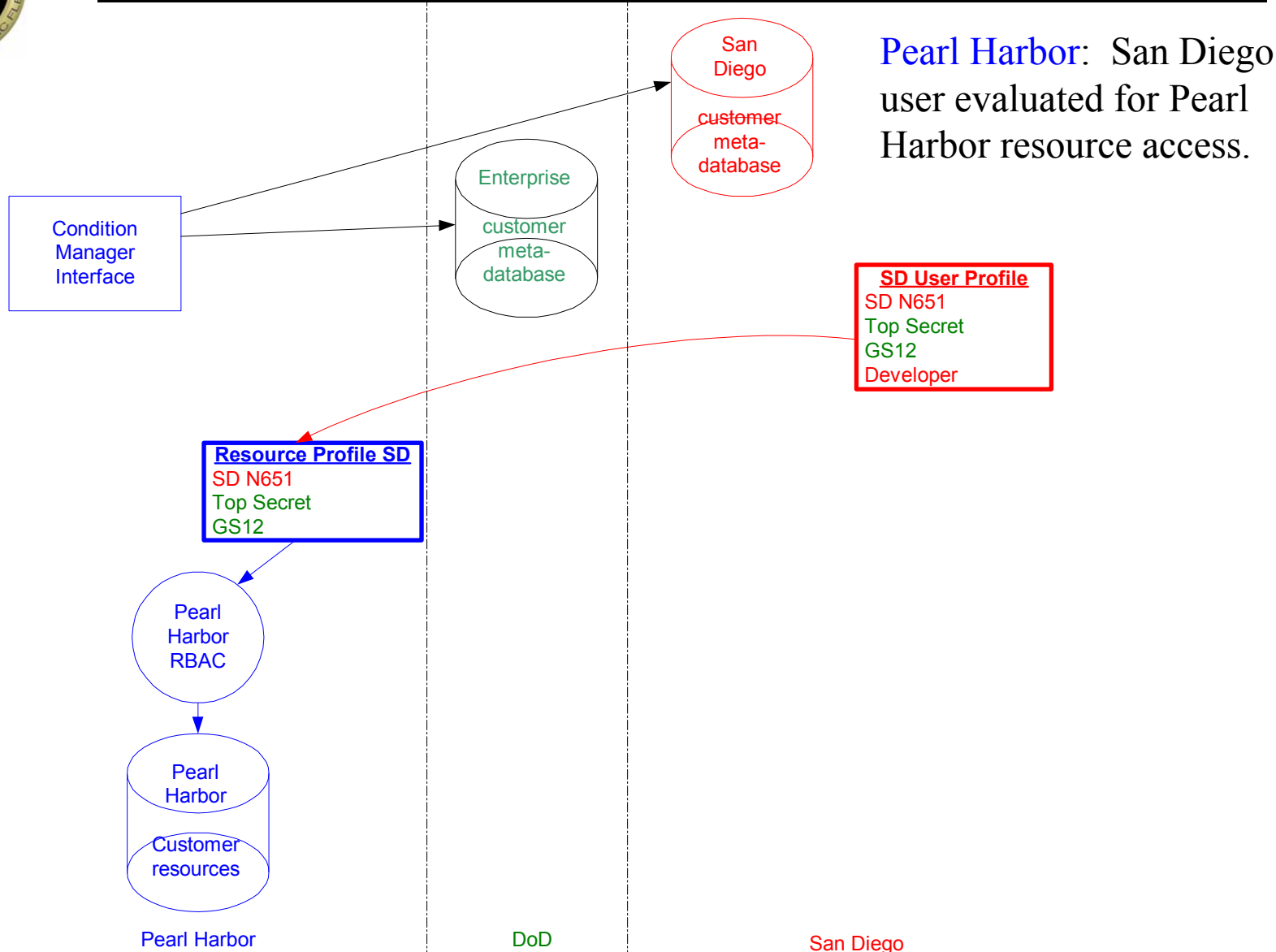
EDAC - Interoperability

San Diego: user profile generated.



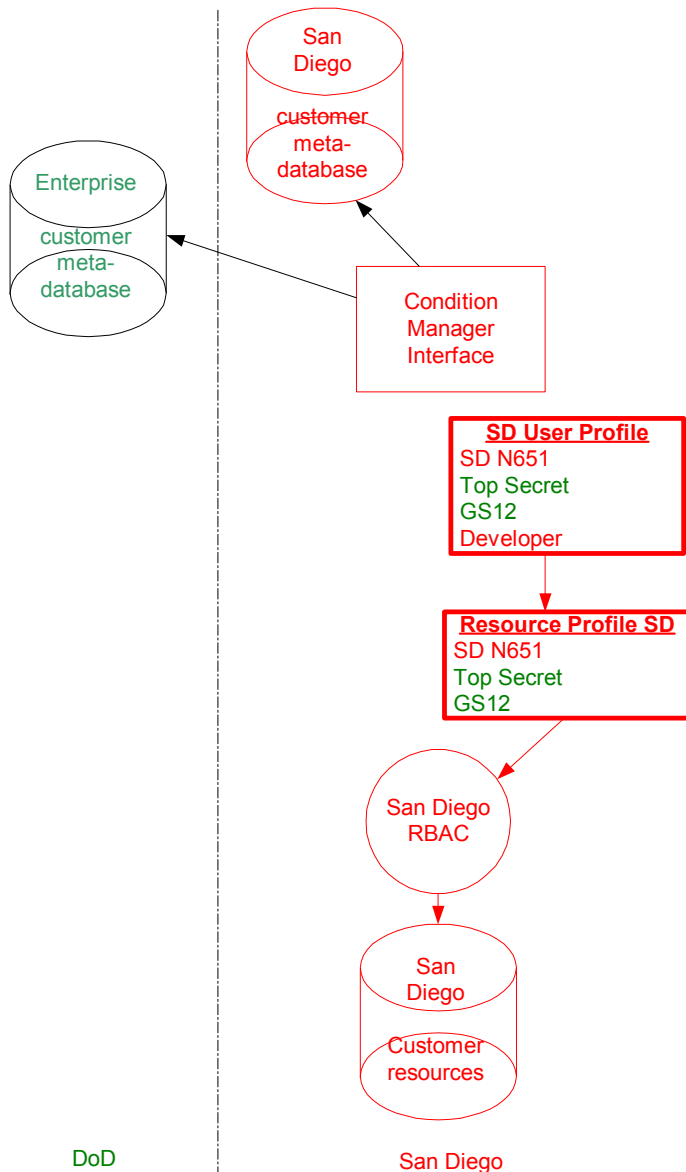


EDAC - Interoperability





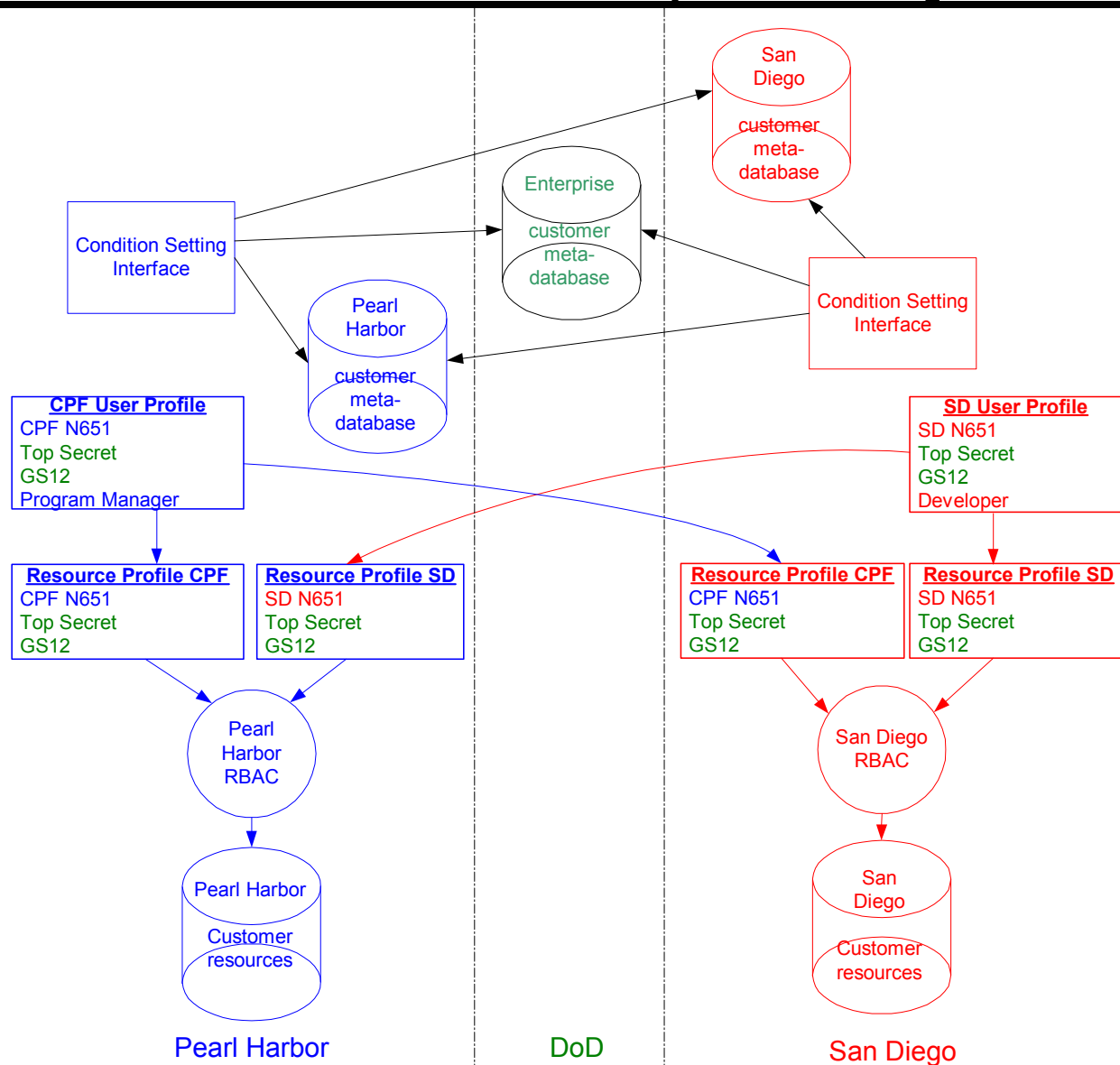
EDAC - Interoperability



San Diego: same user evaluated for San Diego resource access.



EDAC – Interoperability



"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

San Diego, CA 92152-5001

Approved for public release; distribution is unlimited.